RSAC 2025 Conference

Many Voices.
One Community.

SESSION ID: PART2-T02

Five keys to unlocking the potential of AI agents

Dorothy Li
CVP, Microsoft Security Copilot, Ecosystem and Marketplace

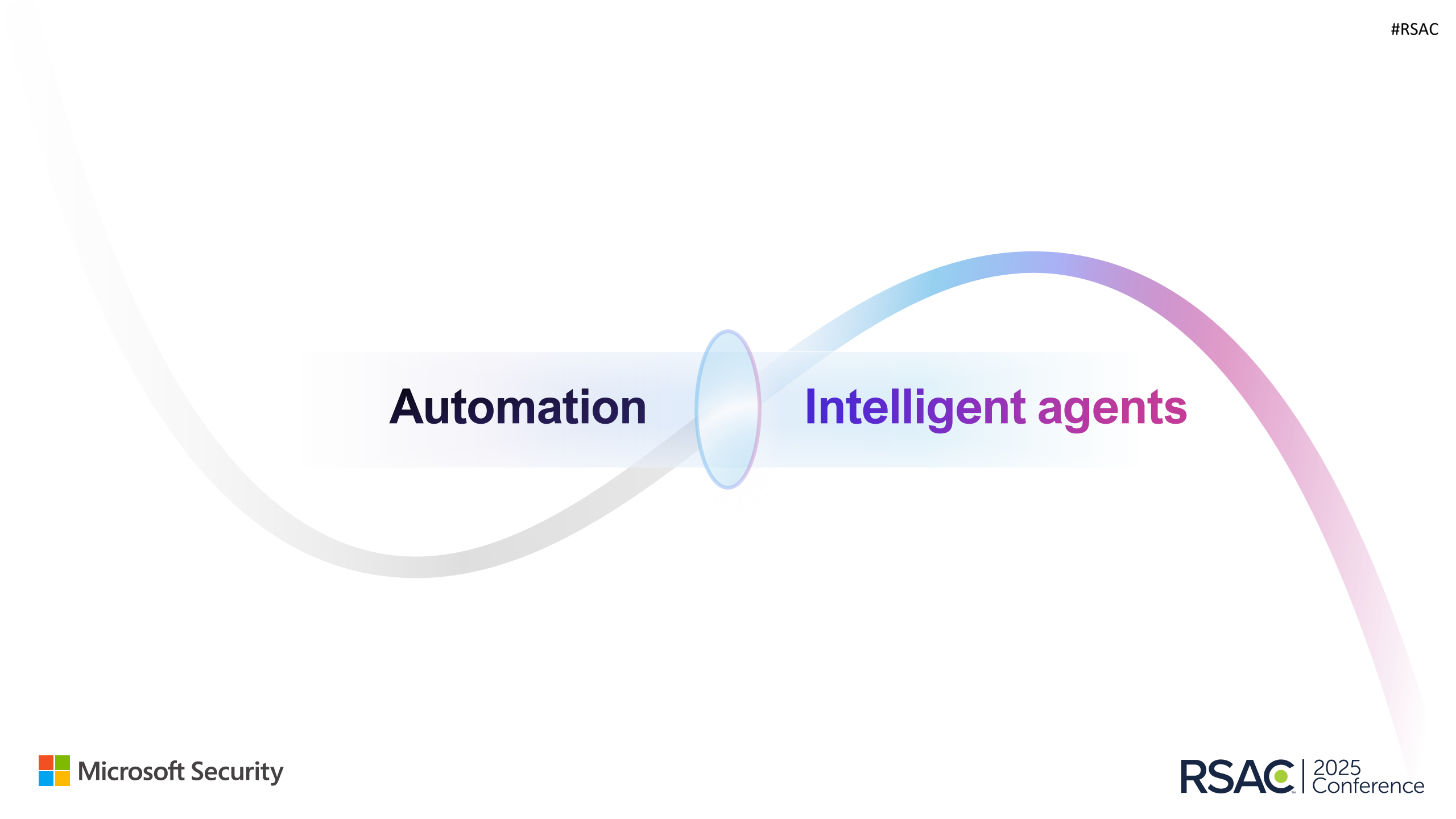
Ryan Munsch
Principal Product Manager
Microsoft Security Copilot

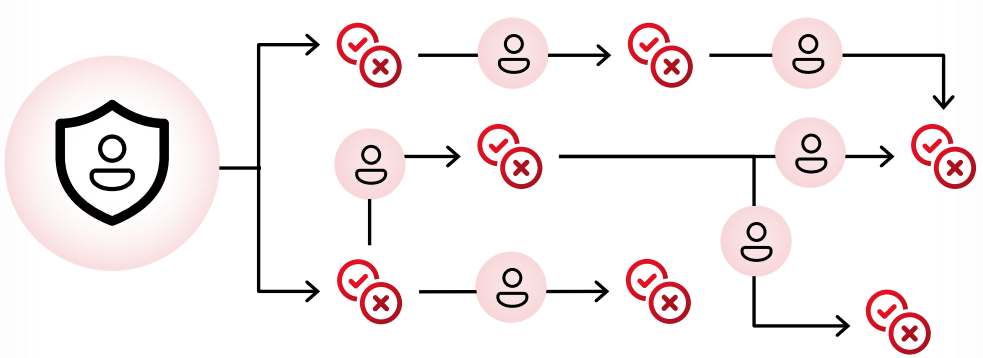
AI

is transforming the security world

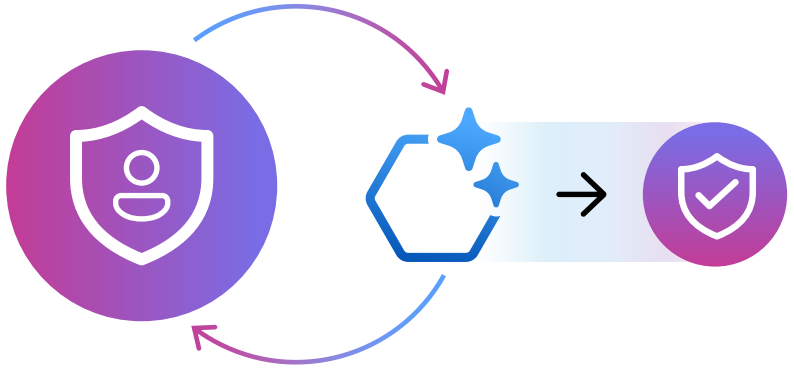
Think, act and work differently

We're at an inflection point


Automation
Intelligent agents



Traditional automation



Agentic AI

Every great shift in technology has redefined how we work

How can we unlock

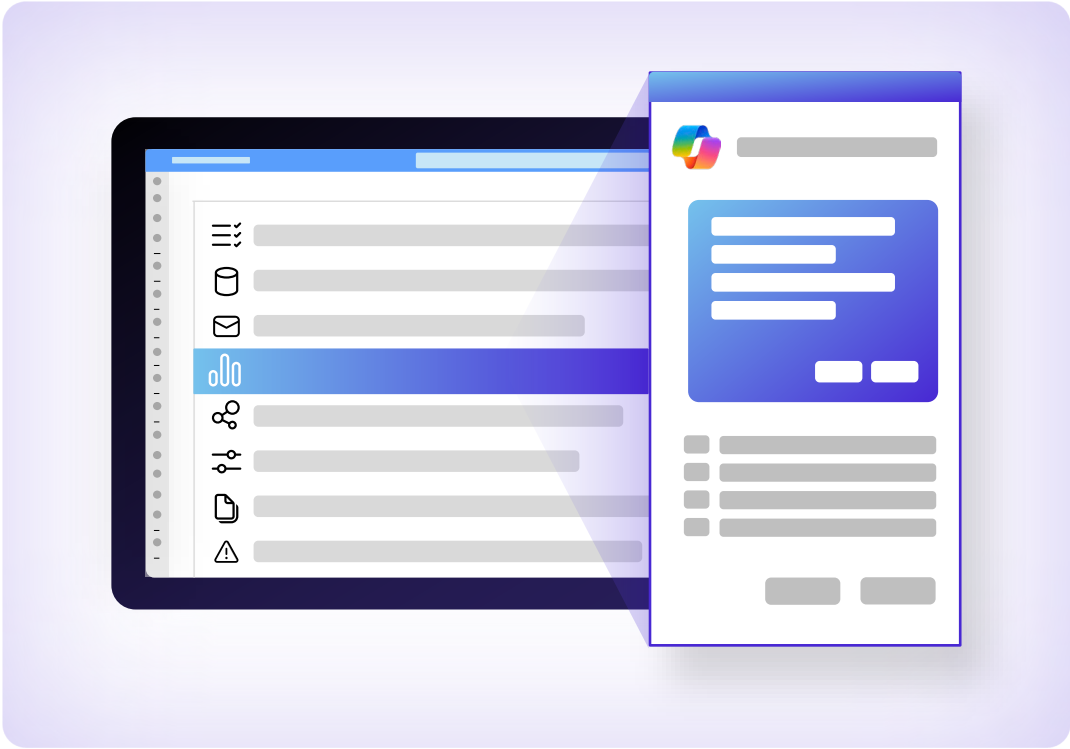
the potential of AI security agents?

Five keys to unlocking the potential of AI agents

1. Empower users where they are
2. Eliminate the drudgery of security
3. Build trust through transparency
4. Shift from reactive to proactive
5. Lead innovation with empathy, not hype

Empower users
where they are

Empower users where they are



Right in the tools they already use

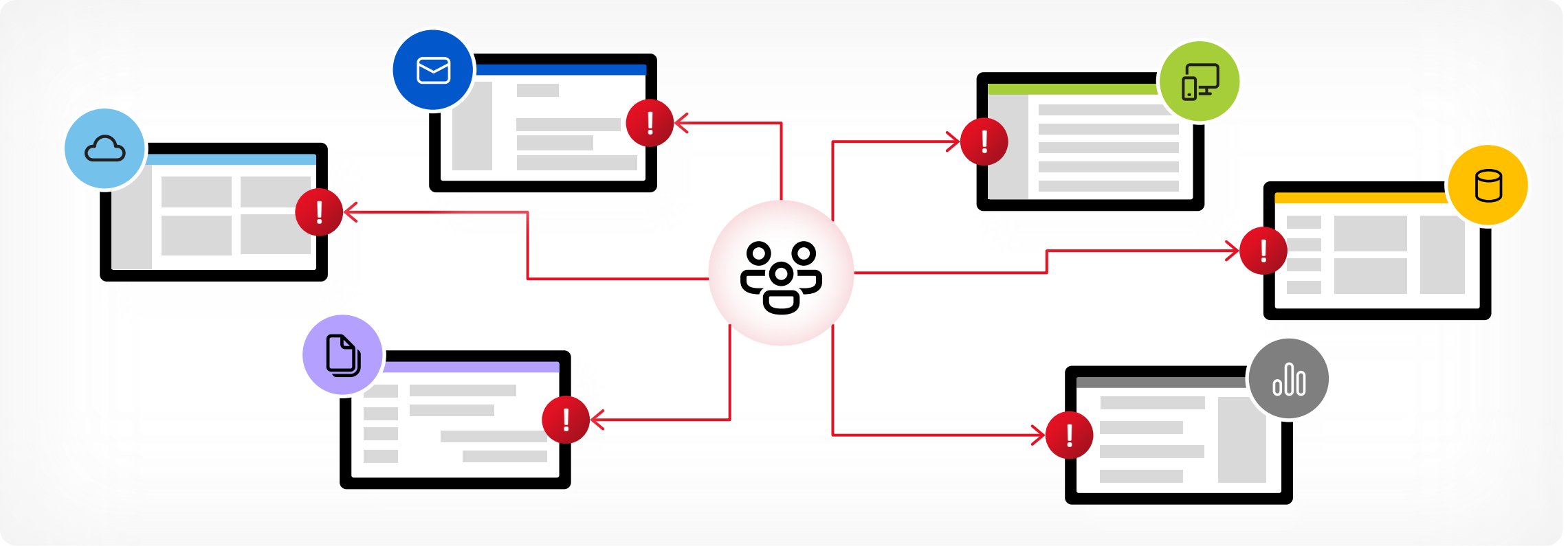
See this in real life:

Agents in your flow, not in your way

of people say context switching makes them less productive

Source: Qatalog and Cornell University's Idea Lab Workgeist Report

Every alert, a new tab.
Every task, a new tool.



Agents in your flow,
not in your way

Meet users where they are

Why it matters?

In a security incident, seconds matter. Agents that stay in your flow improve decision speed, reduce fatigue, and raise adoption.

How to get ahead?

Ask yourself: Can this agent work alongside me in the tools I already use every day?

Agents that appear where analysts live—without added friction—get used more, trusted more, and deliver value faster.

Eliminate the drudgery of security

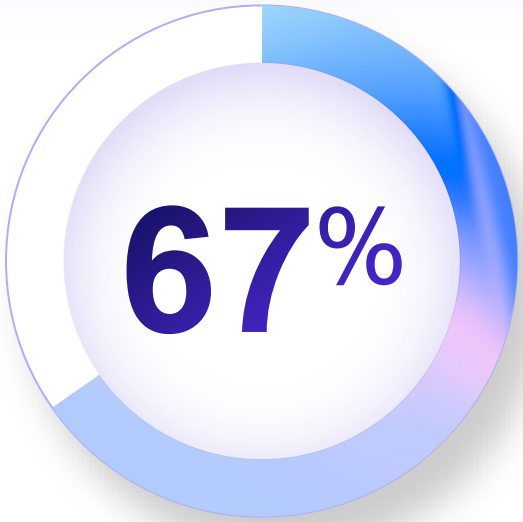
Eliminate the drudgery of security

Endless alerts

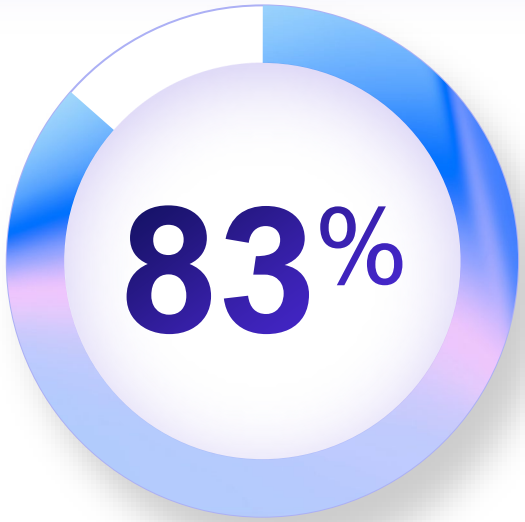
Zero in on critical threats

See this in real life:
Clear the clutter, prioritize the critical

average number of daily alerts for SOC teams



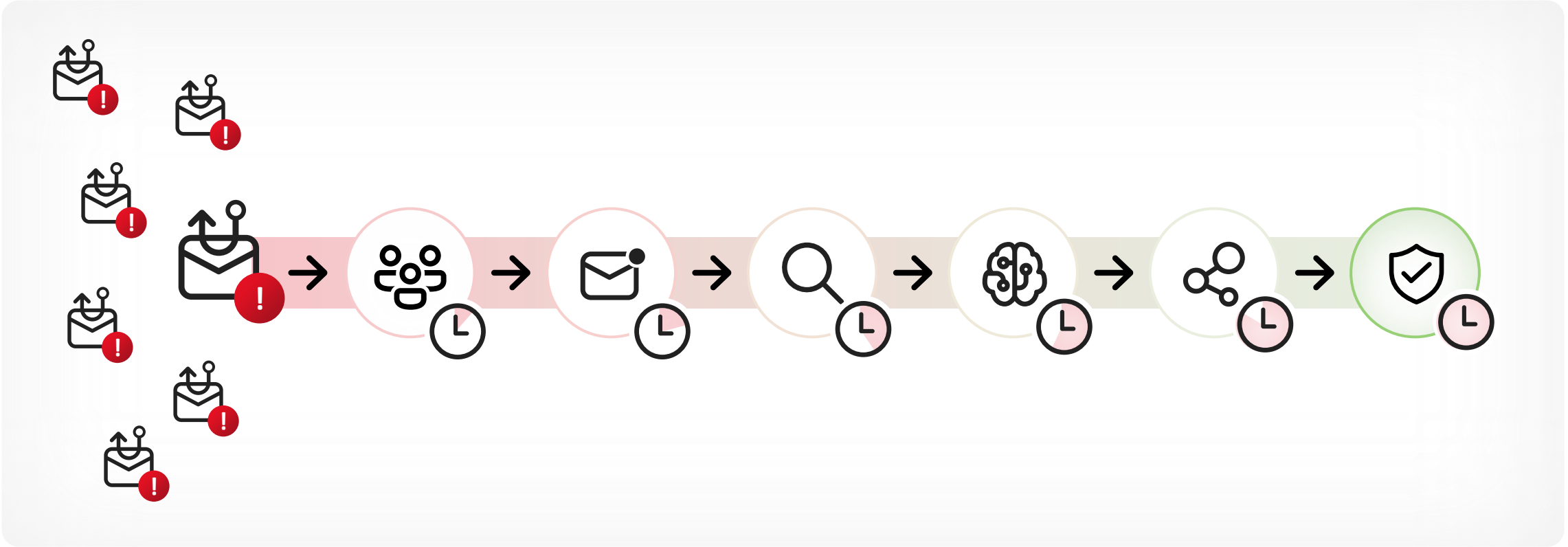
of these alerts are ignored



say these alerts are false positives and not worth their time

Source: 2023 State of Threat Detection Report, Vectra

The anatomy of burnout: A day in phishing triage



Clear the clutter, prioritize the critical

Microsoft Defender XDR

https://security.microsoft.com/agents/phishing-triage-agent/performance

Microsoft Defender

Search

Agents > Phishing Triage Agent

Phishing Triage Agent

Preview

Active

Pause | Edit agent

Overview | Performance | Activity

Last 30 days

Incidents resolved

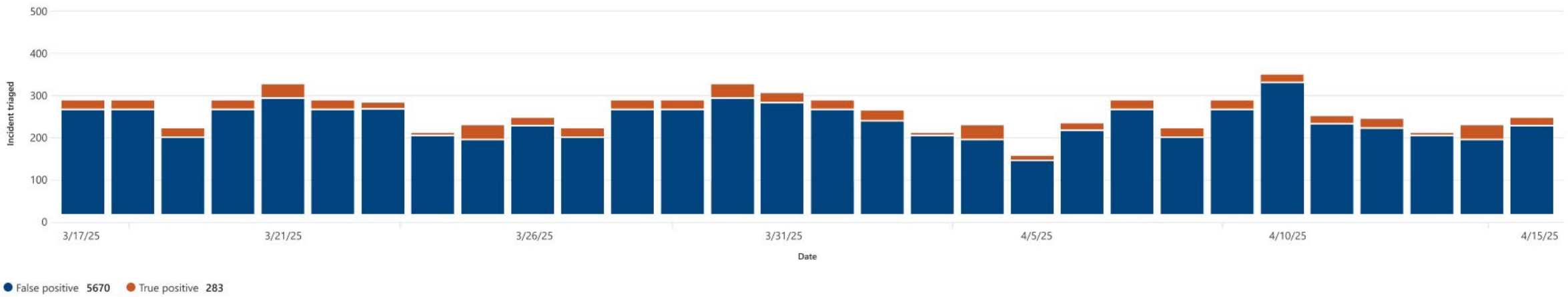
95% (5,670)

Mean time to triage

10min

Incident triage results

See details



Eliminate the drudgery of security

Why it matters?

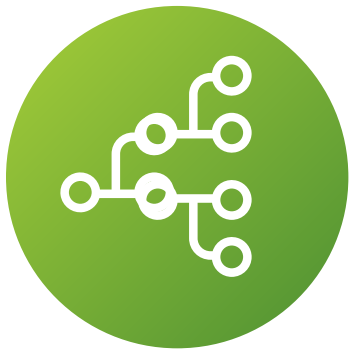
Security agents aren't just smart—they're scalable. Freeing up human time from grind tasks creates room for higher-order thinking.

How to get ahead?

Start with the tasks your team dreads but can't avoid—email triage, false positive review, log summarization. These are prime candidates for agent automation.

Build trust through transparency

Build trust through transparency



Decision tree

Source citations

Human in the loop

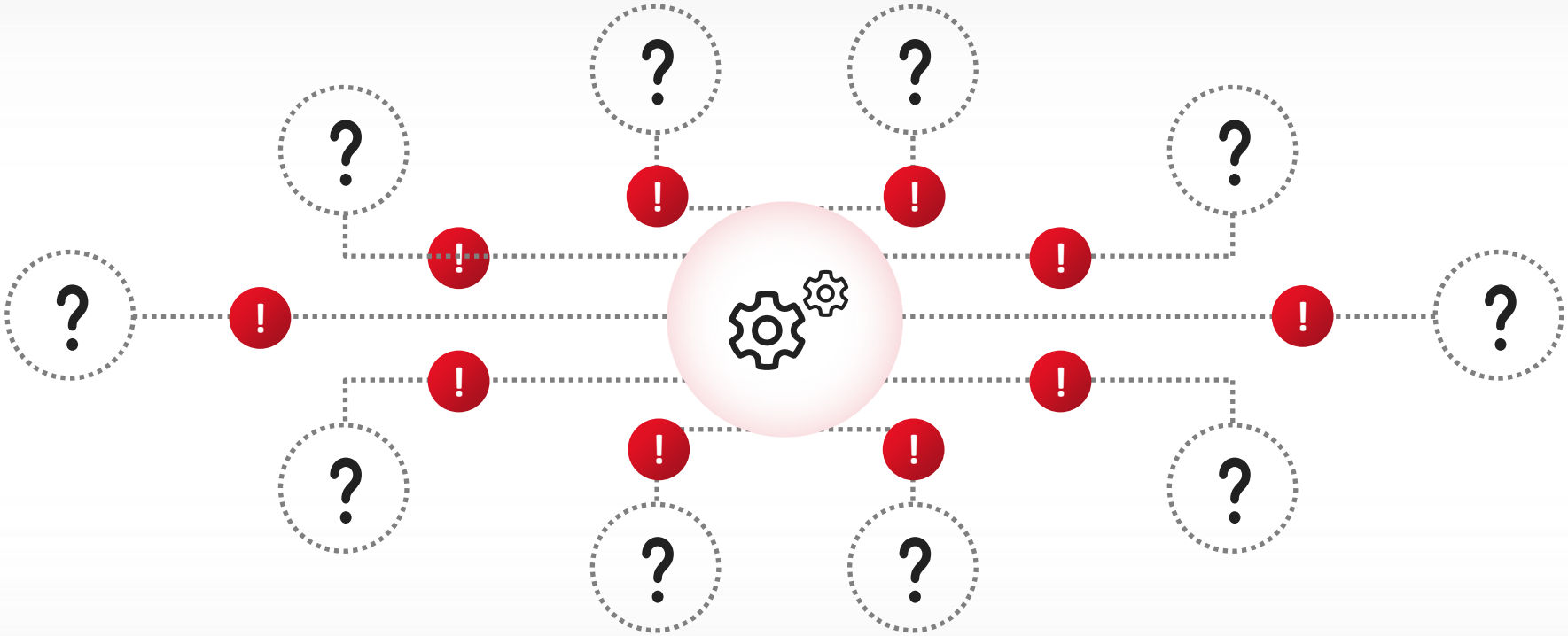
See this in real life:

Total clarity, full control

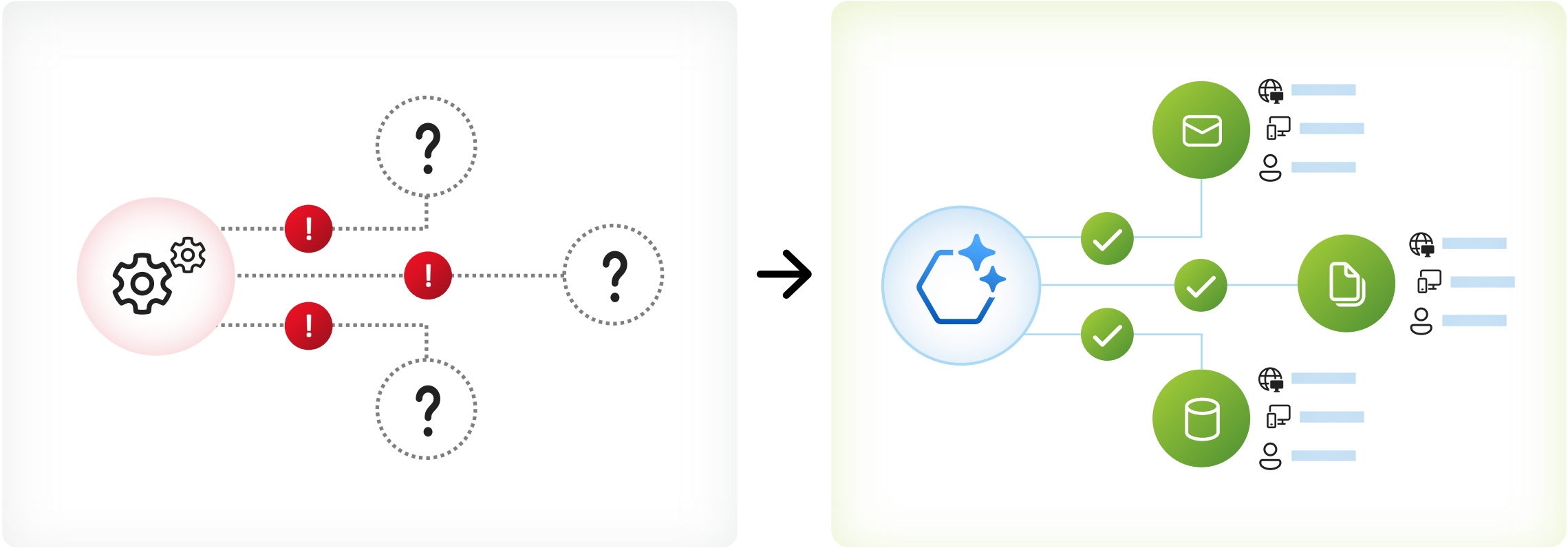
of security professionals trust security findings verified by humans over AI-generated results

Source: WhiteHat The AI and Human Element Security Sentiment Study

The trust gap: When users can’t see the why



Total clarity, full control



Build trust through transparency

Why it matters?

Explainable agents don’t just build trust—they accelerate resolution. You can only act quickly if you understand what you're seeing.

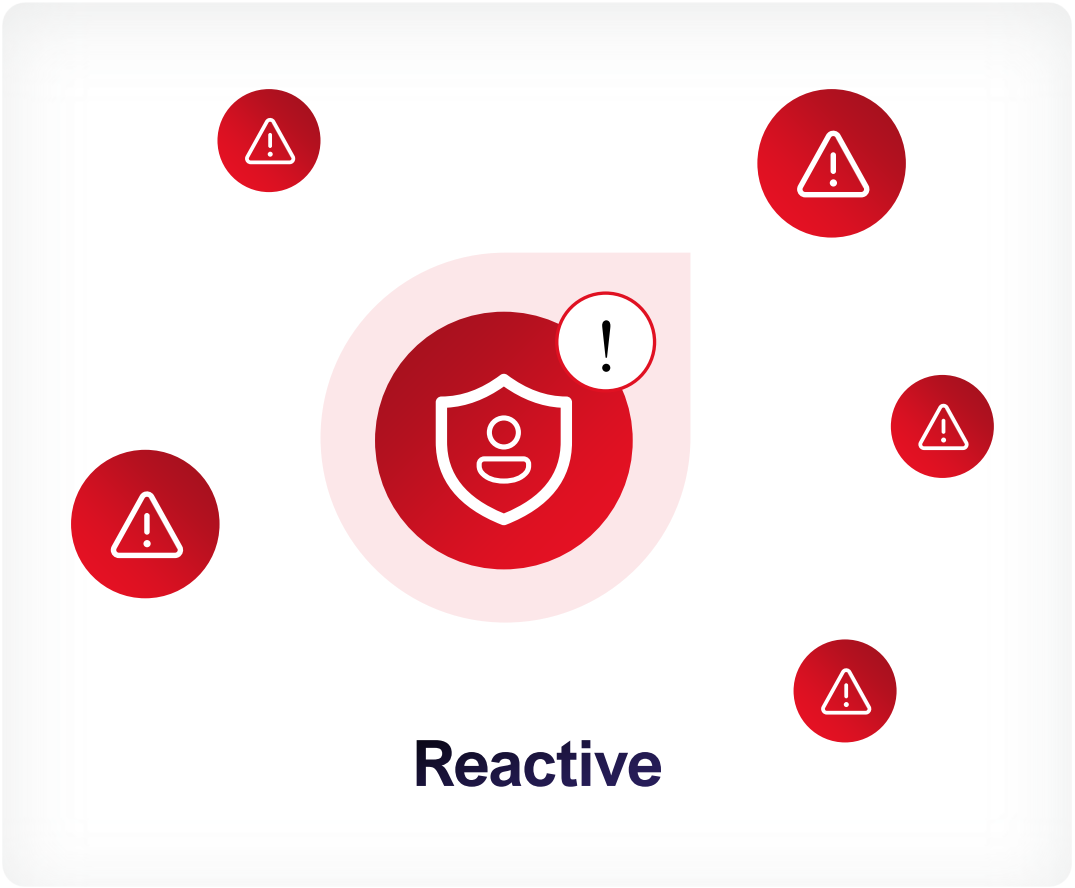
How to get ahead?

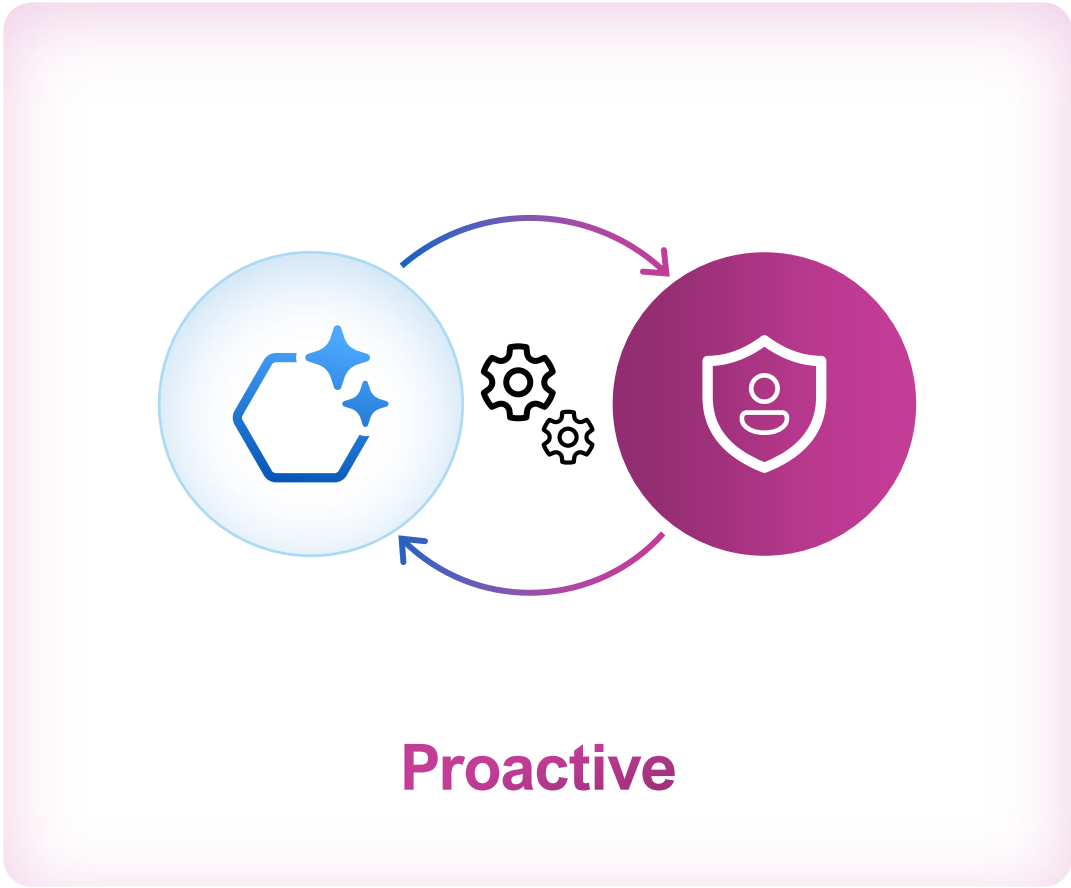
If an agent flags a user as risky, ask: What was seen? What sources were used? How confident is the conclusion?

Great agents don’t just answer—they cite, score, and explain.

Shift from reactive to proactive

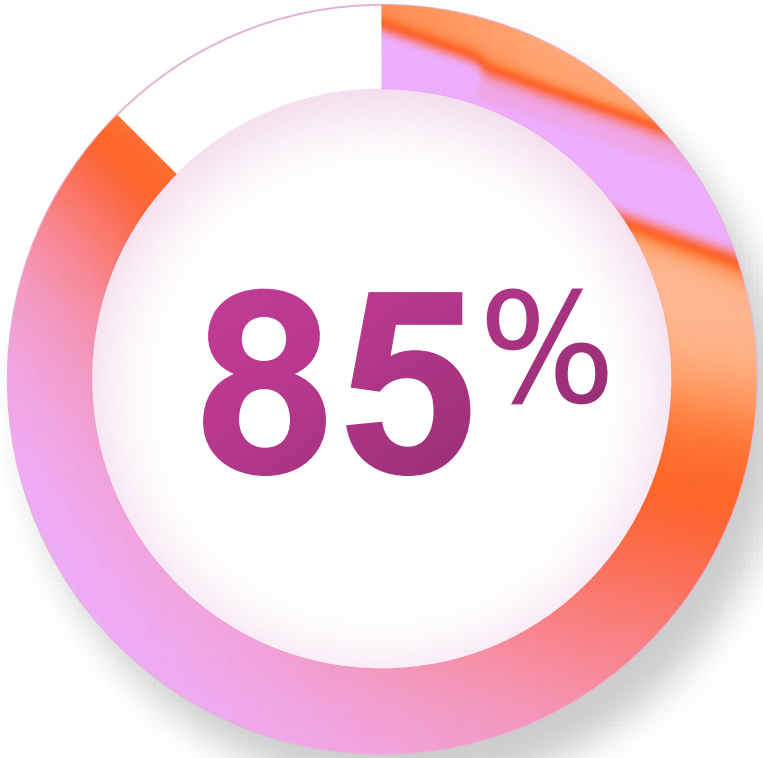
Shift from reactive to proactive





See this in real life:

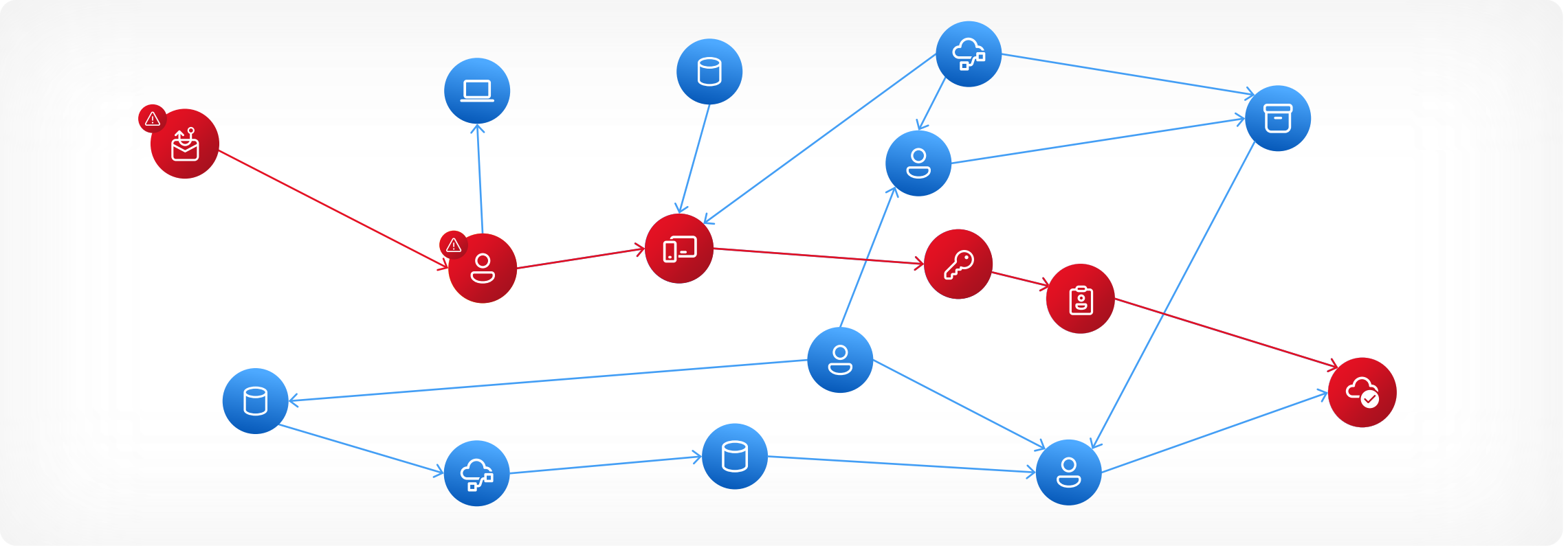
Stay ahead - Scan, prioritize, automate



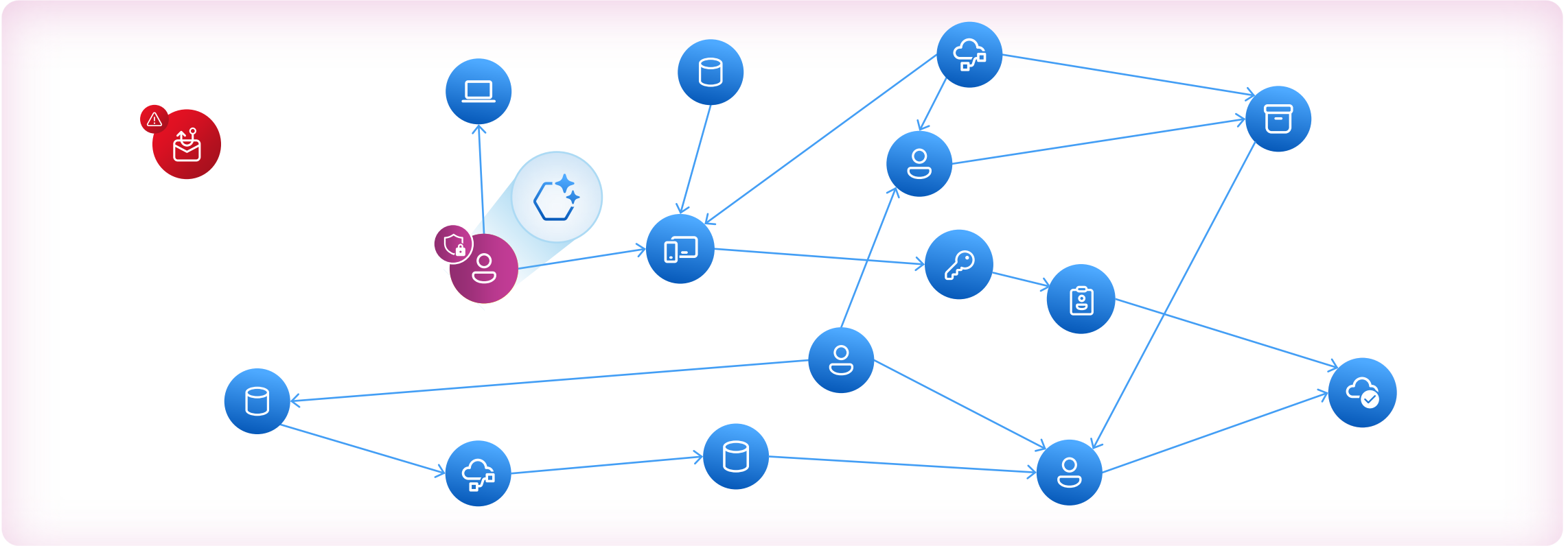
of vulnerabilities remain unpatched after 30 days

Source: Verizon Data Breach Investigations Report 2024

Waiting for the breach to act



Stay ahead:
Scan, prioritize, automate



Shift from reactive to proactive

Why it matters?

Agents that see the weak signals—not just alerts—can change the game. This is how we move from surviving to hardening.

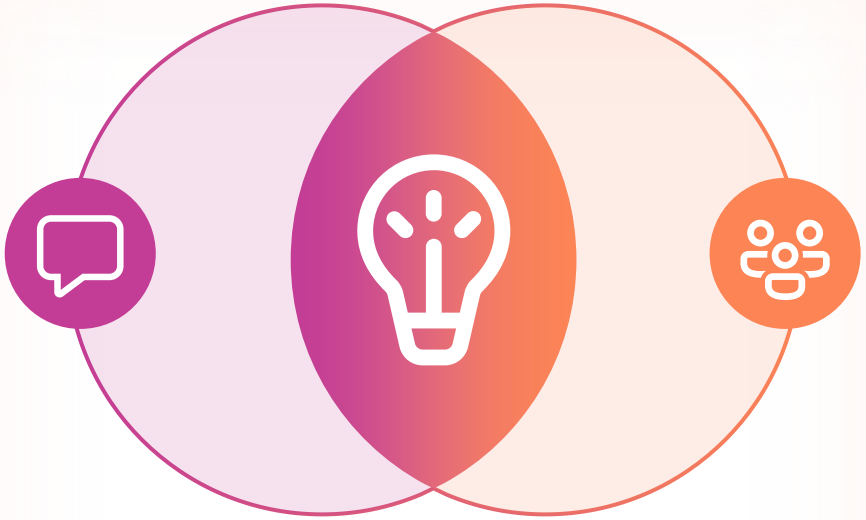
How to get ahead?

Deploy agents that analyze config drift, detect early anomalies, and recommend mitigations. You'll go from chasing alerts to shaping posture.

Lead innovation with empathy, not hype

Lead innovation with empathy, not hype

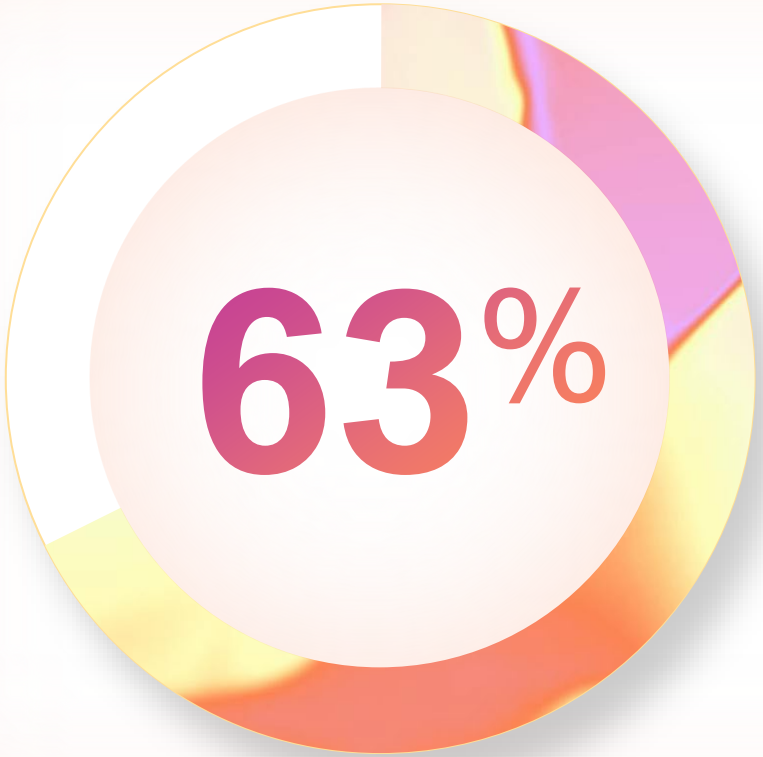
Hype



Empathy

See this in real life:

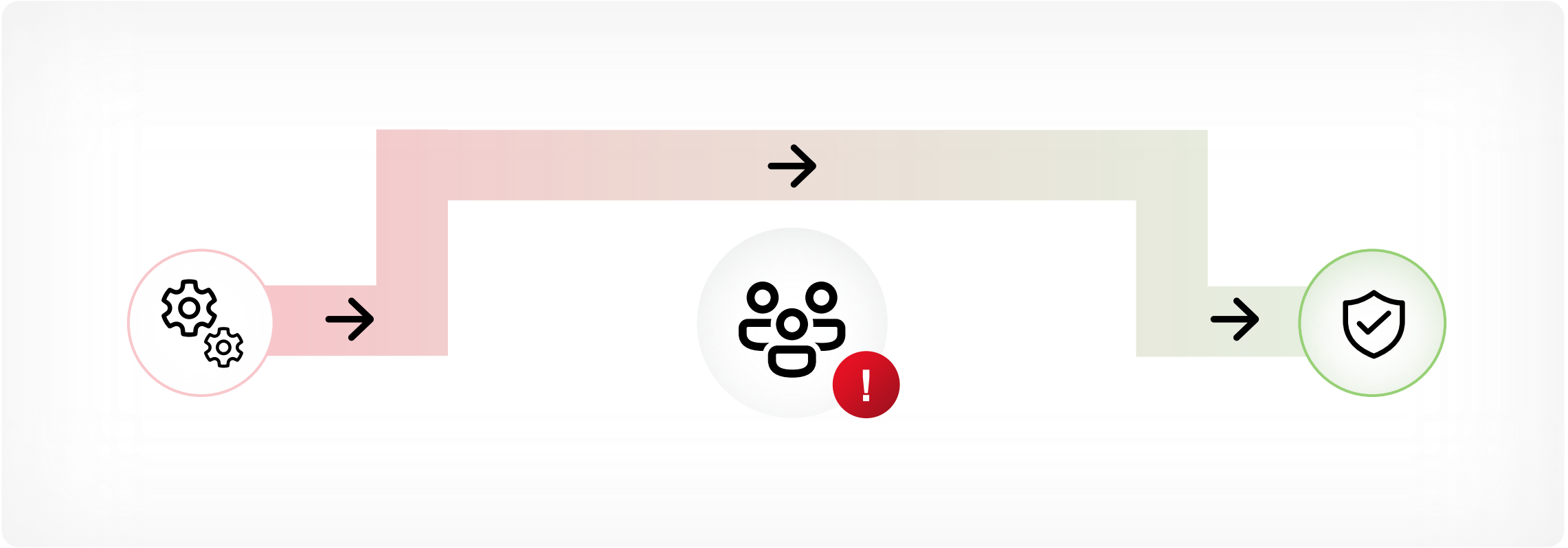
Connecting agents to the people who need them



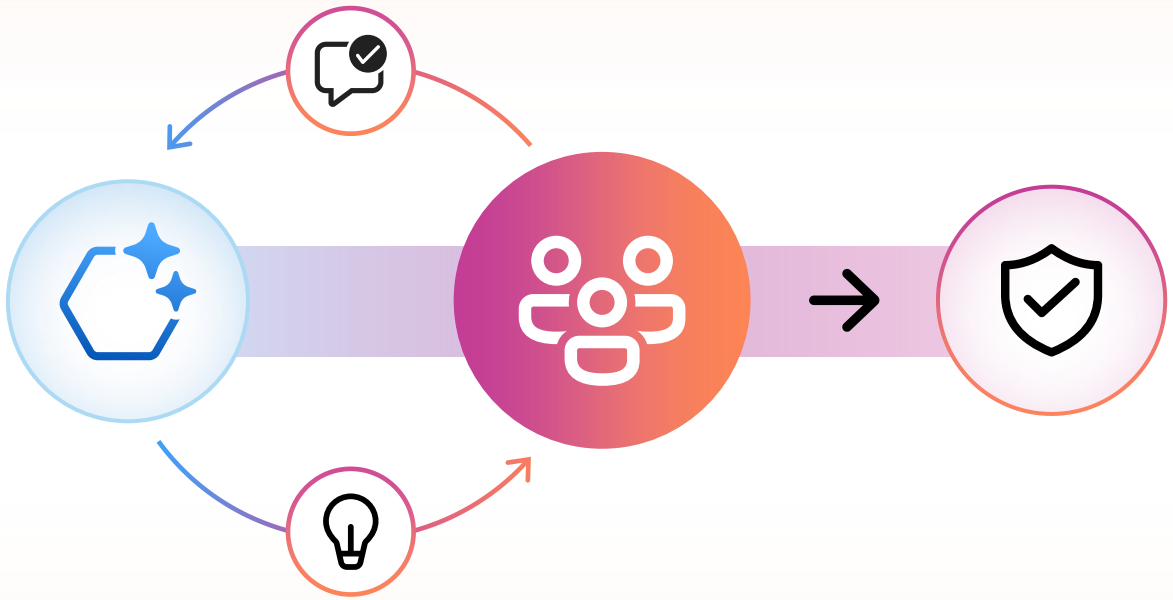
of security professionals believe AI has the potential to enhance security, but as a tool to augment, not replace, human roles

Source: CSA 2024 State of AI and Security Survey Report

Judgment ignored.
Expertise overridden.



Connecting agents
to the people who need them



Lead innovation with empathy, not hype

Why it matters?

Agents that see the weak signals—not just alerts—can change the game. This is how we move from surviving to hardening.

How to get ahead?

Deploy agents that analyze config drift, detect early anomalies, and recommend mitigations. You'll go from chasing alerts to shaping posture.

Five keys to unlocking the potential of AI agents

1 **Meet users where they are**	→ Use agents that work natively across your existing tools and workflows
2 **Eliminate the drudgery of security**	→ Apply agents to high-effort, low-value tasks to free up human focus
3 **Build trust through transparency**	→ Choose agents built with secure, responsible, and human-guided AI
4 **Shift from reactive to proactive**	→ Deploy agents where real-time insights can drive faster decisions
5 **Lead innovation with empathy, not hype**	→ Co-create agent use cases that solve real problems for real teams

RSAC 2025 Conference

Open Q&A

RSAC™ 2025 Conference

Many Voices.
One Community.

Thank you